CLAIMS

What is claimed is:

1. A method for managing the display of sensitive content in non-trusted environments, comprising the steps of:

interrogating a list of policies associated with a given user and a physical device;

determining a location of the physical device;

comparing the location of the physical device with a list of trusted locations; and

enforcing a plurality of rules contained in the policy, wherein access to sensitive information is limited or restricted based on the location.

2. The method of claim 1, wherein the method further comprises the step of providing a reminder to the given user in response to an attempt to access sensitive information on the physical device.

3. The method of claim 1, wherein the method further comprises the step of requesting authentication from the given user in response to an attempt to access sensitive information on the physical device.

4. The method of claim 3, wherein the step of requesting authentication comprises at least one among requesting provision of a unique password for the given user, a unique accessing device, or a unique biometric characteristic of the given user.

5. The method of claim 1, wherein the step of determining a location comprises the step of using at least one among a global positioning system and a terrestrial wireless infrastructure system to provide the location of the physical device.

6. The method claim 1, wherein the step of enforcing comprises at least one among blacking out a display, replacing the sensitive content with innocuous content, prohibiting access to the content, and hiding the content from the given user.

7. A system for managing the display of sensitive content in non-trusted environments, comprising:

a memory;

a display; and

a processor coupled to the memory and the display, wherein the processor is programmed to:

interrogate a list of policies associated with a given user and a physical device;

determine a location of the physical device;

compare the location of the physical device with a list of trusted locations; and

enforce a plurality of rules contained in the policy, wherein access to sensitive information is limited or restricted based on the location.

8. The system of claim 7, wherein the processor is further programmed to provide a reminder to the given user in response to an attempt to access sensitive information on the physical device.

9. The system of claim 7, wherein the processor is further programmed to request authentication from the given user in response to an attempt to access sensitive information on the physical device.

10. The system of claim 9, wherein the processor requests authentication by requesting at least one among the provision of a unique password for the given user, a unique accessing device, or a unique biometric characteristic of the given user.

11. The system of claim 7, wherein the processor determines the location by using at least one among a global positioning system and a terrestrial wireless infrastructure system to provide the location of the physical device.

12. The system of claim 7, wherein the processor enforces the policies by at least one among blacking out a display, replacing the sensitive content with innocuous content, prohibiting access to the content, and hiding the content from the given user.

13. A machine-readable storage, having stored thereon a computer program having a plurality of code sections executable by a machine for causing the machine to perform the steps of:

interrogating a list of policies associated with a given user and a physical device;

determining a location of the physical device;

comparing the location of the physical device with a list of trusted locations; and

enforcing a plurality of rules contained in the policy, wherein access to sensitive information is limited or restricted based on the location.

14. The machine-readable storage of claim 13, wherein the computer program further comprises a plurality of code sections for causing the machine to provide a reminder to the given user in response to an attempt to access sensitive information on the physical device.

15. The machine-readable storage of claim 13, wherein the computer program further comprises a plurality of code sections for causing to request authentication from the given user in response to an attempt to access sensitive information on the physical device.

16. The machine-readable storage of claim 15, wherein the computer program requests authentication by requesting at least one among a provision of a unique password for the given user, a unique accessing device, or a unique biometric characteristic of the given user.

17. The machine-readable storage of claim 13, wherein the computer program determines a location by using at least one among a global positioning system and a terrestrial wireless infrastructure system to provide the location of the physical device.

18. The machine-readable storage claim 13, wherein the computer program enforces the policy by at least one among blacking out a display, replacing the sensitive content with innocuous content, prohibiting access to the content, and hiding the content from the given user.